NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

Nothing Significant to Report

Regional

(Minnesota) **Pelican River's low oxygen levels blamed in fish kill near Orr.** Thousands of fish, including many game fish, died in a fish kill on the Pelican River near Orr, Minnesota, according to a department of natural resources area fisheries supervisor at International Falls, the Duluth News Tribune reported March 20. The kill, probably caused by low oxygen levels in the water, occurred in an approximately 2-mile stretch of the Pelican River from the dam at St. Louis County Highway 23 and downstream past U.S. Highway 53. The fish kill was first reported March 15. A fisheries crew visited the site March 19 and traveled the river by canoe to assess the extent of the kill. "They saw a lot of northern pike, one smallmouth bass, lots and lots and lots of black crappies — probably thousands from 3 inches and up," the supervisor said. "They saw some larger bluegills up to 10 inches, lots of yellow perch and bullheads and suckers." Source: http://www.duluthnewstribune.com/event/article/id/226179/

(Montana) **$10M warrant issued for Bozeman man in int'l Ponzi scheme.** A $10 million arrest warrant was issued for a Bozeman, Montana man wanted for his part in an alleged Ponzi scheme that reportedly defrauded millions of dollars from investors in 20 states and five countries, KBZK 7 Bozeman reported March 22. The suspect faces 20 felony charges that include operating a pyramid scheme, theft by embezzlement, failure to register as a securities salesperson, failure to register a security, and fraudulent practices. Court papers detail many counts of embezzlement. "[He] misled the investors by making untrue statements or omitting material facts when he failed to tell them that he was not investing their money and instead was using it for his Ponzi scheme and/or his own personal use," papers filed in Gallatin County District Court state. One person told officials the man "used his affinity with various ministers, pastors, evangelists and other church-related people ... to solicit investors," court documents state. "A review of the bank records obtained pursuant to the Investigative Subpoena shows that the Defendant and [his wife] received at least $5,388,343 in investment funds from over 140 investors located in Montana, Alabama, Arkansas, California, Colorado, Florida, Georgia, Illinois, Louisiana, Maryland, Michigan, Mississippi, Missouri, New York, North Carolina, Tennessee, Texas, Virginia, Washington, Wisconsin, Canada, Germany, South Korea and Russia," court papers state. The Montana Commissioner of Securities and Insurance (CSI) determined in an investigation that the man misappropriated about $5.4 million and used about $4.4 million of that for his and his wife's own personal use, and the other $1 million or so for his Ponzi scheme. Source: http://www.kxlh.com/news/10m-warrant-issued-for-bozeman-man-in-int-l-ponzi-scheme/

(South Dakota; Midwest) **Repairs needed on river dams.** Among the estimated $10.5 million in repairs planned for Gavins Point Dam near Yanton, South Dakota, is replacing broken or missing cast-iron spillway grates. Twenty are known to be broken or missing and more than 200 others are under water and will be inspected in March. Corps officials have identified 122 repairs to be

done in 2012 following the 2011 flooding. The cost is estimated at more than $186.3 million — plus approximately $54.5 million the following 2 years — at Fort Peck, Garrison, Oahe, Big Bend, Fort Randall, and Gavins Point Dams. Officials primary concerns at Gavins Point include the condition of the spillway's concrete slabs, bank degradation, and restricted flows through the power plant. Peak releases at Gavins Point during the summer-long flood reached 160,000 cubic feet per second — more than twice the previous record, in 1997. High flows scoured away 12 feet of river bottom along a 1,200-yard stretch of the north bank downstream from the dam. That piece of shoreline functions as a dike separating the dam's outflows from Lake Yankton. The lost rock and soil is significant because it could allow seepage from the lake into the river and threaten the dike's integrity. The river side of the dike will be armored with rock the summer of 2012 to prevent future erosion and degradation. Trees and marsh debris coming down Lewis and Clark Lake will plague the Gavins Point power plant for 2 or 3 more years, officials said. Cleanup of the debris is scheduled to begin the week of March 19. Source: http://www.omaha.com/article/20120317/NEWS01/703179897

National

LulzSec announces April Fool's end to retirement. March 17, the hacktivist group formerly known as LulzSec — affiliated with Anonymous and AntiSec — posted a video on YouTube in which they announced they will resume their attacks April 1. The video stated, "Lulzsec will start targeting governments, corporations, agencies, and quite possibly the people watching this video." The announcement was previewed 1 day prior via the FawkesSecurity Twitter channel in a tweet that read, "Expect something BIG and rather Lulzworthy very soon. CIA, FBI, Interpol, you're all on teh (sic) list." March 21, tweets from the same Twitter channel promised "Anonymous will target national infrastructure" and create a "global financial meltdown" as part of what has been dubbed "Project Mayhem." Source: http://www.informationweek.com/news/security/attacks/232602962

IRS needs to further enhance internal control over financial reporting and taxpayer data. The Internal Revenue Service (IRS) implemented many controls and procedures intended to protect key financial and tax-processing systems; nevertheless, control weaknesses continue to jeopardize the confidentiality, integrity, and availability of financial and sensitive taxpayer data processed by agency systems, according to a Government Accountability Office statement March 16. Specifically, the IRS continues to face challenges in controlling access to its information resources. For example, it had not always (1) implemented controls for identifying and authenticating users, such as requiring users to set new passwords after a prescribed period of time; (2) appropriately restricted access to certain servers; (3) ensured that sensitive data were encrypted when transmitted; (4) audited and monitored systems to ensure that unauthorized activities would be detected; or (5) ensured management validation of access to restricted areas. In addition, unpatched and outdated software exposed the agency to known vulnerabilities, and the IRS had not enforced backup procedures for a key system. Source: http://www.gao.gov/assets/590/589399.pdf

INTERNATIONAL

Fukushima farmers face decades of tainted crops as fears linger. Farmers in Japan's Fukushima face years of additional losses as consumers continue to doubt the safety of produce from the region devastated a year ago by the tsunami and nuclear fallout, which may taint crops for decades. Almost 100,000 farmers lost about 58 billion yen ($694 million) by March 1, or 25 percent of production, according to JA, the country's biggest agricultural group. Imports of farm products jumped 16 percent to 5.58 trillion yen in 2011, according to the agriculture ministry. Inadequate testing by the government of rice, milk and fish from the region has prompted consumers to leave them on supermarket shelves and instead select produce from other regions or from overseas. Checks conducted nationwide so far are only 1 percent of what Belarus checked in the past year, a quarter century after the Chernobyl disaster, according to a researcher at Norinchukin Research Institute. Source: http://www.bloomberg.com/news/2012-03-19/fukushima-farmers-face-decades-of-tainted-crops-as-fears-linger.html

BANKING AND FINANCE INDUSTRY

Mousetrap Trojan steals money by chain reaction. The chief security researcher at Bitdefender warned of a new trojan that robs bank accounts. The new Mousetrap campaign starts with a Java applet that has been injected into a popular Web site. This malicious applet, disguised as Adobe Flash Player, warns the user the Flash Player plugin on their computer is outdated and needs an update, but, once executed, the applet downloads and installs another malicious executable file on the machine of the Web site visitor. The attackers likely use 0-day vulnerabilities in blogging Web applications or brute-force weak administrator passwords to add their code in the header file. The downloaded file, written in Visual Basic and packed with UPX, is saved in a writeable location on the user's machine. It downloads and installs a banker from a list (hardcoded in the downloader) of a dozen available links that lead to different banker trojans. To ensure automatic launch, the banker creates a shortcut to itself. Each time the system starts, all programs with shortcuts added in that folder are automatically initiated as well, including the banker. Once on the system, the banker updates itself by downloading newer versions from a second list of links. The updates are hosted on multiple servers so that if one is shut down, the rest can still be accessed. The banker Trojan feeds users with a log-in form and asks them to fill it in. The data entered by the unwary clients is intercepted by crooks and sent to a C&C server. Source: http://www.net-security.org/malware_news.php?id=2044&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+(Help+Net+Security)&utm_content=Google+Reader
http://www.net-security.org/malware_news.php?id=2044&utm_source=feedburner&utm_med-###

Linkedin e-mail scam deposits banking trojan. GFI Labs recently discovered a LinkedIn e-mail phishing scam that installs the Cridex banking Trojan. The fake LinkedIn e-mail looks like an authentic e-mail reminder about pending invitations. The phishing scam shares the same IP address (41.64.21.71) as several recent Better Business Bureau and Intuit spam runs. The Cridex bot, also known as Cardep or Dapato, was discovered in the wild in August 2011. It spreads

through e-mailed or shared attachments. Once installed, the trojan connects to a remote command and control (C&C) server. Then it injects itself into the target's Internet Explorer process, where it steals online banking credentials, e-mail accounts, cookies, and FTP credentials, and sends them back to the C&C server. Earlier this month, M86 Labs reported that Cridex currently infects 25,000 machines. Source: http://securitywatch.pcmag.com/security/295538-linkedin-email-scam-deposits-banking-trojan

Polish authorities seize $100 million in fake US treasury bonds, arrest 8 people. Eight people are to be questioned on counterfeiting charges March 19 after they were found with $100 million in fake U.S. treasury bonds in their possession, Polish authorities said. The central anti-corruption bureau, a state agency, said the suspects — three Poles, two Italians, two Ukrainians, and a Moldovan woman — were arrested March 18 in regions around Krakow and Lublin, in southern and eastern Poland. A bureau spokesman said the value of the fake bonds was a record seizure for the bureau. No other details were immediately available, and it was not clear if any fake bonds in the scam made it to the market. Source: http://www.washingtonpost.com/world/europe/polish-authorities-seize-100-million-in-fake-us-treasury-bonds-arrest-8-people/2012/03/19/gIQA3gybMS_story.html

Chemical and Hazardous Materials Sector

EPA proposes significant new use rules, test regulation for variety of chemicals. The Environmental Protection Agency (EPA) proposed a package of rules March 20 that would require chemical producers and other manufacturers to notify it before they make, import, or process a variety of chemicals, including certain flame retardants, in ways the agency would designate as new uses. The package consists of six elements: proposed revisions to existing significant new use rules (SNURs) covering a group of flame retardants called polybrominated diphenyl ethers (PBDEs) and existing SNURs for benzidine-based dyes; newly proposed SNURs for hexabromocyclododecane, or HBCD, a flame retardant, a phthalate called di-n-pentyl phthalate (DnPP), and one type of short-chain chlorinated paraffin called alkanes, C12-13, chloro; and a proposed test rule for PBDEs that would be coupled with the agency's proposed amended significant new use rules for those flame retardants. Companies that import the seven PBDEs or nine benzidine-based dyes as part of "articles" — products such as furniture or electronics — would be covered by the SNURs addressing those chemicals. The rules emerged from a series of action plans the agency has issued since December 2009. Source: http://www.bna.com/epa-proposes-significant-n12884908483/

New labeling rules aim to protect workers from hazardous chemicals. The U.S. President's administration is adopting long-awaited rules to improve labels on hazardous chemicals and make them conform with international guidelines developed by the United Nations, the Associated Press reported March 20. The Occupational Safety and Health Administration (OSHA) estimated that such labels could prevent more than 40 deaths and about 500 workplace injuries and illnesses from exposure to hazardous chemicals each year. About 43 million U.S. workers come in contact with hazardous materials on the job. Development of the rules began during the previous President's administration, and they were initially proposed in 2010. The

current Presidential administration said the move now is part of a presidential directive in 2011 to streamline burdensome rules and eliminate red tape. Chemical manufacturers currently have to produce two sets of labels and records: one to satisfy U.S. standards and another to meet the U.N. guidelines. OSHA officials said that by ending the duplication, the industry could save more than $475 million annually in training costs and paperwork. Source: http://www.washingtonpost.com/politics/new-government-safety-rules-aim-to-protect-workers-from-hazardous-chemicals/2012/03/20/gIQACnzXPS_story.html

(Colorado) **Fracking wells' air emissions pose health risks, study finds.** Chemicals released into the air when natural gas is produced by hydraulic fracturing may pose a health risk to those living nearby, the Colorado School of Public Health said in a new report. Researchers found potentially toxic airborne chemicals near wells in Garfield County, Colorado, during 3 years of monitoring. Emissions from the wells include methane and volatile organic compounds that react with heat and sunlight to form ozone, according to a health scientist with the Environmental Defense Fund. The U.S. Environmental Protection Agency has proposed rules that would reduce oil and gas well emissions. The research focused on those living about a half mile from the wells and was requested by county officials in response to the rapid expansion of fracking in the state. One operator has proposed drilling 200 wells about 500 feet from homes in Garfield County. Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/g/a/2012/03/19/bloomberg_articlesM14RQV6JTSEC01-M153F.DTL

Commercial Facilities

(California) **Arsonist sets multiple fires within 90 minutes.** The Bakersfield Fire Department believes one man set several arson fires within an hour and a half March 19 in northeast Bakersfield, California, setting ablaze different things in different locations. Security cameras at a Farmer Boys restaurant filmed the arsonist as he set fire to a dumpster behind the business. "He goes back and looks into a dumpster, and it appears he's setting up the boxes that we have back there in our trash bins and walks away. As soon as he does, you see white smoke coming up and in seconds it starts flaming up," the restaurant's manager said. Police are currently looking for a suspect based a description from the video footage. Source: http://www.turnto23.com/east_county/30717835/detail.html

Communications Sector

DOJ sues AT&T, alleging improper billing of services for hearing impaired. The U.S. Department of Justice (DOJ) said March 22 it has sued AT&T Inc. on allegations the telecommunications giant improperly billed the Federal Communications Commission (FCC) for services it provided to the hearing-impaired. The lawsuit, brought under the federal False Claims Act, is focused on AT&T's providing of a text-based communications service that allows the hearing-impaired to place telephone calls by typing messages over the Internet. The DOJ said AT&T sought FCC reimbursement for services it provided to international callers who were ineligible for the service and sought to use it for fraudulent purposes. The government alleges AT&T received "millions" from the improper billing. Source:

http://www.nasdaq.com/article/doj-sues-att-alleging-improper-billing-of-services-for-hearing-impaired-20120322-00839

'Hacktivists' steal more than 100M online records in 2011, says Verizon. More than half of data stolen from companies in 2011 was a result of hacktivist actions, even though the majority of data breaches were still caused by financially motivated cybercriminals, Verizon said in its 2012 Data Breach Investigations Report released March 22. The report spans 855 data breach incidents investigated by the company and several law enforcement agencies. These incidents resulted in 174 million compromised records, the second-highest volume of compromised records since Verizon began compiling data breach statistics in 2004. Up to 98 percent of data breach incidents covered by the new report were caused by external agents and the vast majority of them, 83 percent, were organized criminal groups. Hacktivists were responsible for only 3 percent of data breaches. However, they had the biggest impact in terms of compromised records, over 100 million of the 174 million. Source: http://www.computerworld.com/s/article/9225425/_Hacktivists_steal_more_than_100M_online_records_in_2011_says_Verizon?taxonomyId=17

Virgin Mobile USA hit by national data, SMS outage. Virgin Mobile USA was recovering March 21 from a national outage that left customers across the country without data or text messaging service. The network problems were confirmed by the prepaid provider in posts on its Twitter and Facebook accounts the afternoon of March 20. "We are currently experiencing a national data & text messaging outage," the company said on its Facebook page. A company spokeswoman said March 21 that the interruption in service has since been resolved and the problem stemmed from one of its servers. "We did have some issues related to a server," she said. "In most cases, it required customers to remove their battery and restart device." Virgin Mobile is one of Sprint's prepaid brands, and runs its voice, data, and SMS service on Sprint's CDMA EV-DO network. Neither Sprint nor its prepaid brand Boost Mobile has reported any issues. However, Assurance Wireless, another Sprint brand operated by Virgin Mobile, told a customer on its Facebook page who was having problems with text service that "we were experiencing a 3G/MMS/SMS outage yesterday." Source: http://www.wirelessweek.com/News/2012/03/networks-Virgin-Mobile-Hit-By-Outage/

Critical Manufacturing

Nothing Significant to Report

Defense/ Industry Base Sector

Ex-gov't scientist gets 13 years in espionage case. A former government space scientist was sentenced March 21 to 13 years in prison after admitting he tried to sell space and defense secrets to Israel in what turned out to be an FBI sting operation. Prosecutors and the scientist's lawyers agreed to the 13-year sentence, with credit for 2 years he has spent behind bars since his arrest. The scientist had high-level security clearances during decades of government work on science and space projects at NASA, the Energy Department, and the National Space Council

during the 41st presidential administration. He pleaded guilty to one count of attempted espionage, admitting he tried to provide Israel with top secret information about satellites, early warning systems, methods for retaliating against large-scale attack, communications intelligence information, and major elements of defense strategy. Source: http://www.businessweek.com/ap/2012-03/D9TL50J02.htm

U.S. nukes face up to 10 million cyber attacks daily. According to U.S. News and World Report March 20, the computer systems of the agency in charge of America's nuclear weapons stockpile are "under constant attack" and face millions of hacking attempts daily, said officials at the National Nuclear Security Administration (NNSA). The head of the agency said it faces cyber attacks from a "full spectrum" of hackers. "They're from other countries' [governments], but we also get fairly sophisticated non-state actors as well," he said. "The [nuclear] labs are under constant attack, the Department of Energy is under constant attack." A spokesman for the NNSA said the Nuclear Security Enterprise experiences up to 10 million "security significant cyber security events" each day. "Of the security significant events, less than one hundredth of a percent can be categorized as successful attacks against the Nuclear Security Enterprise computing infrastructure," the spokesman said — which puts the maximum number at about 1,000 daily. The agency wants to increase its cybersecurity budget from about $126 million in 2012 to about $155 million in 2013 and developed an "incident response center" responsible for identifying and mitigating cybersecurity attacks. Source: http://www.usnews.com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily

Raytheon's $621 million halted by U.S. on missile delays. The U.S. Air Force is withholding $621 million in payments to Raytheon Co., the biggest U.S. maker of missiles for the U.S. military, citing chronic delays in delivering the most advanced air-to-air missile for the service and the U.S. Navy, Bloomberg reported March 20. Raytheon's Missile Systems unit, based in Tucson, Arizona, was 193 missiles behind schedule as of February 29, according to Air Force data. The Air Force notified Raytheon March 3 it was withholding $419 million in fiscal 2010 payments. That is in addition to $202 million the service was already withholding for 2007 to 2009. Alliant Techsystems Inc., Raytheon's subcontractor, "has had difficulty for the past year consistently producing rocket motors to specification," according to the Air Force. The missiles are the newest version of the Advanced Medium-Range Air-to-Air Missile. They are intended for deployment to Air Force fighter wings and Navy aircraft carriers once testing is done and they are declared combat-ready in fiscal 2013, the service said. Source: http://www.bloomberg.com/news/2012-03-20/raytheon-s-621-million-halted-by-u-s-on-missile-delays.html

Spies target Taiwan's U.S.-made defenses. Taiwanese security personnel detained a suspected spy for China at a top secret military base that utilizes sensitive U.S. technology in February, the Associated Press reported March 21. The air force captain was the fourth Taiwanese in 14 months known to have been picked up on charges of spying for China. While Taiwan's defense ministry did not disclose details of the alleged offense, his base in the northern part of the island hosts the air force's highly classified radar system and U.S.-made Patriot surface-to-air

missiles. The captain's arrest followed that of a major general, who had access to crucial information on Taiwan's U.S.-designed command and control system, and a civilian, who the defense ministry says tried without success to inveigle Patriot-related secrets from an unnamed military officer. A fourth alleged spy was detained on non-defense-related charges. The cases show China is seeking data about systems integral to Taiwan's defenses and built with sensitive U.S. equipment. Information about the defense systems could also help the People's Liberation Army understand other U.S. defenses. Source: http://militarytimes.com/news/2012/03/ap-china-spies-target-taiwan-us-made-defenses-032112/

Emergency Services

(Pennsylvania) **More than 200 Pa. transit cops on strike.** More than 200 Southeastern Pennsylvania Transit Authority (SEPTA) police officers went on strike March 21, after announcing a stalemate in contract talks with the transit authority. Members of the Fraternal Order of Transit Police, Local 30, who have worked without a contract for nearly a year, walked off the job. SEPTA and the Philadelphia Police Department immediately implemented a contingency plan to provide security for city riders. The transit agency said it also was coordinating with suburban police departments, Amtrak, PATCO, the University of Pennsylvania, and Temple University. The union decided to go on strike after both sides refused to come to an agreement on pay raises based on the officers' police certifications. A SEPTA spokesman declined to discuss details of the negotiations, but said that what the union was seeking was out of line with what the agency had agreed to with its other unions. Source: http://www.officer.com/news/10666468/more-than-200-pa-transit-cops-on-strike

(California) **California struggles to set up early quake warning system.** California has struggled to build and deploy an earthquake warning system that would give cities time to prepare for the impact of a massive earthquake, the Los Angeles Times reported March 21. California is spending only a fraction of what other countries have devoted, and scientists said the progress is so slow they cannot say when the state might complete its system. One reason for the lack of interest, some experts said, is that unlike Mexico, Japan, and the other countries with early warning systems, California has not experienced a truly catastrophic earthquake in more than a century. Officials in California have been working on a system for about 5 years. Alerts of coming earthquakes in California could be sent via Twitter and other forms of social media, with scientists hoping to get out word as broadly as possible. Alerts also would go up on TV and radio. With the warning, scientists hope that emergency crews would have time to open fire station doors, protect nuclear power plants, slow down trains, and take other measures before the quake would be felt. Source: http://www.latimes.com/news/local/la-me-03-22-quake-warning-20120322,0,7059435.story

Energy

MIT research: Study finds room to store CO2 underground. A new study by researchers at the Massachusetts Institute of Technology (MIT) March 19 shows there is enough capacity in deep saline aquifers in the United States to store at least a century's worth of carbon dioxide

emissions from the nation's coal-fired power plants. One of the most promising places to store the gas is in deep saline aquifers: those more than half a mile below the surface, far below the freshwater sources used for human consumption and agriculture. However, estimates of the capacity of such formations in the United States have ranged from enough to store just a few years' worth of coal-plant emissions up to many thousands of years' worth, according to the report. The MIT team modeled how the carbon dioxide would percolate through the rock, accounting not only for the ultimate capacity of the formations but the rate of injection that could be sustained over time. Source: http://www.eurekalert.org/pub_releases/2012-03/miot-mrs031912.php

Audit: Gas lines tied to fracking lack oversight. Government auditors said federal officials know little about thousands of miles of pipelines that carry natural gas released through the drilling method known as fracking, and need to step up oversight to make sure they are running safely, the Associated Press reported March 23. Amid the gas-drilling boom, private companies have put in hundreds of small gathering pipelines to collect new fuel supplies released through the high-pressure drilling technique. Nationwide, about 240,000 miles of gathering pipelines ferry the gas and oil to processing facilities and larger pipelines in the major energy-producing states. Many of these pipelines course through densely populated areas, including neighborhoods in Fort Worth, Texas. The Government Accountability Office said in its report issued March 22, that most of those miles are not regulated by the U.S. Pipeline and Hazardous Materials Safety Administration, which means they are not regularly inspected for leaks or corrosion. In some states, officials do not know where the lines are. Nationwide, there are about 200,000 miles of gas-gathering lines and up to 40,000 miles of hazardous liquid gathering lines in rural and urban areas alike, ranging in diameter from about 2 to 12 inches. But only about 24,000 of those miles are regulated, according to the report. Source: http://www2.wsav.com/news/2012/mar/23/audit-gas-lines-tied-to-fracking-lack-oversight-ar-3462008/

U.S. studies vulnerability of fuel pipelines to East Coast. The United States is studying the vulnerability of Colonial Pipeline Co. and Kinder Morgan Energy Partners LP pipelines that carry fuel from Gulf of Mexico refineries to the East Coast, the DHS said March 19. "We will be conducting analysis to better understand how disruptions to Colonial's pipeline and Plantation pipelines could affect the broader critical infrastructure," said the director of the department's Homeland Infrastructure Threat and Risk Analysis Center. "Our primary concern would be a prolonged damage to the pipeline that kept it down more than a week, more than 2 weeks," the director said. "Once you start getting beyond a week or two, the ability for the excess inventory at terminals along its route starts to be diminished and then you start to have more serious impacts." Source: http://www.bloomberg.com/news/2012-03-19/u-s-studies-vulnerability-of-fuel-pipelines-to-east-coast-1-.html

Food and Agriculture

Foot and mouth outbreak in Egypt threatens region, UN's FAO says. A major outbreak of foot-and-mouth disease in Egypt is threatening the North Africa and Middle East regions, the United

Nations' (UN) Food and Agriculture Organization (FAO) reported on its Web site March 22. Egypt suspects 40,222 cases of the livestock disease, and 4,658 animals have already died, the Rome-based FAO wrote, citing official estimates. The strain of the disease is new, meaning livestock have no immune protection against it, according to the UN agency. Source: http://www.businessweek.com/news/2012-03-22/foot-and-mouth-outbreak-in-egypt-threatens-region-un-s-fao-says

USDA warns of fraudulent letters. The U.S. Department of Agriculture (USDA) said someone is faxing fraudulent letters to people and businesses in Wisconsin and other states, the Associated Press reported March 19. The letters claim to come from a USDA procurement officer and seek personal information. They have the USDA logo and seal and are signed by a man using the title "senior procurement officer." The false letters have been faxed to Wisconsin, Alabama, Nebraska, and Pennsylvania, and may have been sent to other states. Source: http://www.claimsjournal.com/news/national/2012/03/19/203180.htm

Insecticides linked to honeybee die-offs. Die-offs of honeybees critical for pollinating food crops — part of so-called colony collapse disorder — is linked to an insecticide, according to a U.S. journal, United Press International reported March 15. Researchers from the University of Padua in Italy writing in the journal Environmental Science & Technology said the springtime die-offs were linked to technology used to plant corn coated with insecticides. In some parts of Europe where farmers use the technology to plant seeds coated with so-called neonicotinoid insecticides, widespread deaths of honeybees have been reported since the introduction of the technique in the late 1990s, they said. Such insecticides are among the most widely used in the world, popular because they kill insects by paralyzing nerves but have lower toxicity for other animals. Scientists said they suspected the bee die-offs might be due to particles of the insecticide made airborne by the pneumatic drilling machines used for planting that forcefully suck seeds in and expel a burst of air containing high concentrations of particles of the insecticide coating. Source: http://www.upi.com/Technology_News/2012/03/15/Insecticides-linked-to-honeybee-die-offs/UPI-96311331840460/?spt=mps&or=5

Allergen alert: Caramel 'Puffcorn' snack with milk. Troyer Cheese, Inc. is recalling their Backroad Country Caramel Puffcorn, because it may contain undeclared milk, Food Safety News reported March 18. This recall was discovered when the milk-containing product were distributed in packaging that did not have a label saying the presence of milk in the ingredient statement. "Backroad Country Caramel Puffcorn" is sold in 8- and 16-ounce plastic bags and was distributed between January 6 and March 12 in 32 states in retail stores and through mail orders. Distribution of the product has been suspended until the Food and Drug Administration and the company are certain the problem is corrected. Source: http://www.foodsafetynews.com/2012/03/allergen-alert-caramel-puffcorn-snack-with-milk/

(California) **Chicken wraps recalled for undeclared allergens.** LSG Sky Chefs is recalling about 1,784 pounds of grilled chicken Caesar wraps because the Caesar dressing used contains egg, a known allergen not declared on the wrap product label, Food Safety News reported March 18. The company is recalling packages of "7-Eleven Fresh to Go Grilled Chicken Caesar Wrap" with a

"Freshest Before" packaging date of March 15 through March 18. The products were produced from March 12 and March 15, have a 2 day shelf-life, and were distributed to 7-Eleven stores in northern California. The problem was discovered by the company during a routine label review. Source: http://www.foodsafetynews.com/2012/03/chicken-wraps-recalled-for-undeclared-allergens-1/

Canada recalls seven months worth of frozen ground beef. After a series of earlier recalls, the Canadian Food Inspection Agency (CFIA) recalled all ground beef from New Food Classics processed between July 1, 2011 and February 15 because it may be contaminated with E. coli O157:H7. One person was reportedly sickened after eating meat processed in October 2011. New Food Classics went into receivership in February, according to the Toronto Star. The company packaged burgers and steakettes under brand names including Best Value, Loblaws' no name, no name Club Pack, Country Morning, and Grillhouse. According to the court filing, the Saskatchewan-based company learned February 15 its frozen ground beef was linked to a case of E. coli O157:H7 illness and 3 days later recalled 3,800 cases of frozen burgers. Another 767 cases were recalled February 22. All together, about 1.25 million cases of ground beef products were taken off the market. CFIA, in a news release the weekend of March 17, warned the public not to consume the company's frozen ground beef products, and also warned all retailers, distributors, and restaurants not to sell, serve, or use these ground beef products. The beef was distributed nationally in Canada. Source: http://www.foodsafetynews.com/2012/03/canada-calls-back-seven-months-of-frozen-ground-beef/

Glass fragments in fruit beverages. The Canadian Food Inspection Agency and AllJuice International are advising customers not to consume certain AllJuice products because they may contain harmful glass fragments, Food Safety News reported March 19. The recalled juices were distributed in Ontario, Canada, and include: Alljuice Key Lime Fruit Beverage, Alljuice Strawberry Kiwi Fruit Beverage, Alljuice Cranberry-Raspberry Cocktail Fruit Beverage, Alljuice Mango Fruit Beverage, and St. Maarten Mangos & Carrots Fruit Beverage. Source: http://www.foodsafetynews.com/2012/03/glass-fragments-in-fruit-beverages/

Uninspected pork recalled. Lawson Foods of Irvington, New Jersey, is recalling about 84,587 pounds of pork that includes pork imported from Canada not properly presented for re-inspection upon entry into the United States, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced March 19. FSIS said the shipment of imported pork, inspected and passed by the Canadian authorities, arrived from Canada earlier than scheduled and and was sold to Lawson Foods without being presented to U.S. food safety authorities for re-inspection. The recall is for various weight cases of PORK SHOULDER BUTTS. This product was produced March 3 and was distributed to one wholesale firm in New Jersey. Source: http://www.foodsafetynews.com/2012/03/uninspected-pork-recalled/

Stink bugs threaten crops in U.S. South. Two Mid-Atlantic hurricanes last year had the effect of pushing that region’s invasive stink bug infestation into the deep south, U.S. Department of Agriculture scientists say. The Washington Post reported March 16 the brown marmorated

stink bugs have headed south from Pennsylvania, Maryland, and West Virginia into South Carolina, Georgia, and Florida, putting vegetable and citrus crops at risk. Another type of stink bug is damaging soybeans and other legumes in Georgia. In 2010, they caused about $37 million in damage to mid-atlantic apple crops alone. Peach and raspberry crops also took heavy hits in some parts of Maryland. Agriculture officials worry it could get worse once the bugs become established in Florida. Source: http://www.upi.com/Science_News/2012/03/17/Stink-bugs-threaten-crops-in-US-South/UPI-74531332034124/

Government Sector (including Schools and Universities)

OMB: Growth in federal cyberattacks slows. NextGov reported March 16 that cyberattacks on the U.S. government continue to increase, but most were "phishing" attempts and reports of threats largely leveled out in the past year, according to the Office of Management and Budget (OMB). OMB reported a 5 percent increase in cyberattacks on federal networks in 2011, based on reports to the U.S. Computer Emergency Readiness Team. That is compared to a 39 percent spike in such attacks the previous fiscal year. "Threats to this IT infrastructure — whether from insider threat, criminal elements, or nation-states — continue to grow in number and sophistication, creating risks to the reliable functioning of our government," the report concluded. Of the total 107,655 attacks reported in 2011, 43,889 were aimed at federal departments and agencies. Source: http://www.nextgov.com/nextgov/ng_20120316_7803.php

FBI says retaliation attacks possible in US. An FBI spokeswoman in Seattle said the agency and the DHS issued a bulletin March 15 to raise awareness about the possibility of homegrown extremist retaliation in response to the killings of civilians in Afghanistan. A soldier from Joint Base Lewis-McChord near Tacoma, Washington, was accused of the shootings. The spokeswoman said there was no specific target or credible information about an imminent attack. However, she said the FBI has previously seen extremists plot attacks in retaliation for the actions of soldiers. They include a plot last year to attack a military recruit processing station in Seattle. Source: http://seattletimes.nwsource.com/html/localnews/2017762767_apwaafghanistanretaliation.html

AF's delicate rescue saves stranded $1.7B satellite. U.S. Air Force ground controllers rescued a $1.7 billion military communications satellite last year that had been stranded in the wrong orbit and at risk of blowing up — possibly because a piece of cloth had been left in a critical fuel line during manufacture, the Associated Press reported March 19. During the 14-month effort, the satellite had to battle gravity and dodge space junk while controllers improvised ways to coax it more than 21,000 miles higher to its planned orbit. "This rescue effort was definitely a very sophisticated and highly technical masterpiece," said the chief of the Military Satellite Communications Division at Peterson Air Force Base, Colorado. The Advanced Extremely High Frequency (AEHF) satellite is the first of six in a $14 billion communications system. Lockheed Martin, expected to build all six AEHF satellites, said the probable cause was a foreign object

that got into the system during manufacture. The Air Force said the next two AEHF satellites have been inspected and additional checks have been added to the manufacturing process for the remaining versions. Source: http://www.military.com/news/article/af-delicate-rescue-saves-stranded-17-billion-satellite.html

US govt. and military e-mail addresses offered for sale. Webroot recently unearthed an offer for sale of millions of e-mail addresses harvested by a cybercrime underground service, which has cleverly segmented the database based on country or generic top-level domains, Help Net Security reported March 19. "Next to mass marketing campaigns, the segmented databases could be used for launching targeted attacks against a particular country, which in combination with localization — translating the spam message into the native language of the prospective recipient — and event-based social engineering attacks, could increase the probability of successful interaction with the malicious e-mails," a security expert at Webroot said. He also advised U.S. government and military users to be especially careful when considering the legitimacy of received e-mails, as among the e-mail addresses offered for sale are over 2 million on .gov and .mil domains. Source: http://www.net-security.org/secworld.php?id=12611

Information Technology and Telecommunications

ISPs commit to new cybersecurity measures. March 22, a group of U.S. Internet service providers (ISPs) committed to taking new steps to combat three major cybersecurity threats based on recommendations from a U.S. Federal Communications Commission (FCC) advisory committee. The ISPs, including AT&T, Comcast, Time Warner Cable, and Verizon Communications, committed to implement measures to fight botnets, domain name fraud, and Internet route hijacking. The FCC's Communications, Security, Reliability, and Interoperability Council (CSRIC) also adopted the recommendations for voluntary action by ISPs March 22. Eight wired and wireless ISPs, representing about 80 percent of the broadband subscribers in the United States, are members of CSRIC and signed on to the recommendations. Source: http://www.computerworld.com/s/article/9225446/ISPs_commit_to_new_cybersecurity_measures?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+(Computerworld+Security+News)&utm_content=G

Flash-based rogue AV targets users. In a recently discovered spam e-mail campaign promoting fake AV, the links in the messages take users to one of more than 300 compromised domains. Once users lands on the page, a JavaScript message warning about a "critical process activity" prepares them for a fake scan which immediately starts "running." "The page uses Flash making it look more convincing with realistic icons, progress bars, and dialog boxes," according to the researchers. "Unsurprisingly, the fake antivirus detects plenty of viruses. Decompressing the Flash file and analyzing it shows a huge list of files contained within it. The Flash movie then simply picks some of these at random and claims they are infected (with equally random virus names)." Users are then offered the option of removing all the found malware. If they choose not to, they are bombarded with warnings about an imminent system crash and urged to change their decision. If they choose to remove the malware, they are offered a "Windows Risk Minimizer" for downloading and, once run, the fake solution appears legitimate. It also runs a

scan and finds the system is overrun with malware. If users still fail to proceed to buy a subscription for the solution and close the window, the fake AV will vex them with pop-up warnings and balloon messages indicating a program was blocked from stealing data, identity theft is in process, or threats of prosecution. It then claims the problems can be solved by buying a lifetime subscription and support for the fake AV for $99. Source: http://www.net-security.org/malware_news.php?id=2046&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+(Help+Net+Security)&utm_content=Google+Reader

IBM warns hackers wising up to firms' security policies. Hackers are adapting to the security policies firms are putting in place to steal corporate data and infiltrate systems, according to new research by IBM. The firm made the warning in its X-Force 2011 Trend and Risk Report, which explored the public vulnerability disclosure findings from over 4,000 clients. The report also warned there was a marked increase in the number of attacks targeting mobile devices and social networks. Notably, the authors reported a 19 percent rise in publicly-released mobile exploits, indicating hackers are increasingly targeting mobile devices as they grow in prominence in the work place. An X-Force strategy and threat intelligence manager said the growing bring your own device trend in many companies posed several risks by making it hard for IT staff to ensure employees devices are correctly patched with the latest security software, offering a potential goldmine of unsecured personal information to hackers. The report also warned attacks taking place on social media sites are also increasing, with many hackers using such sites to help develop new techniques to steal data. IBM also warned that cloud computing is a major security issue, because some companies pushed the technology out without taking adequate measures to protect the stored data.Source: http://www.v3.co.uk/v3-uk/news/2162563/ibm-warns-hackers-wising-firms-security-policies

Most web masters don't know how their sites got hacked, report says. Most owners of compromised Web sites do not know how their sites got hacked into, and only 6 percent detect the malicious activity on their own, according to a report released March 22. The new "Compromised Websites: An Owner's Perspective" report is based on a survey of more than 600 Web site administrators and owners that was carried out over several months by security vendor Commtouch, and StopBadware, a nonprofit organization that helps Web masters identify, remediate, and prevent Web site compromises. The leading cause of compromises appears to be outdated content management software. This was cited as a reason for Web sites being hacked by 20 percent of respondents. Twelve percent of Web masters said a computer used to update their Web site was infected with malware, 6 percent said their credentials were stolen credentials, and 2 percent admitted logging in while using wireless networks or public PCs. However, 63 percent of respondents did not know how their Web sites were compromised. Source: http://www.computerworld.com/s/article/9225442/Most_web_masters_don_t_know_how_their_sites_got_hacked_report_says?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+computerworld/s/feed/topic/17+(Computerworld+Security+News)&utm_

Experts tell Senate: Government networks owned, resistance is futile. Network security experts from across the U.S. government told a U.S. Senate Armed Services subcommittee March 20 federal networks have been thoroughly penetrated by foreign spies and current perimeter-based defenses that attempt to curb intrusions are outdated and futile. Speaking before the Senate Armed Services Subcommittee on Emerging Threats and Capabilities, the experts said the U.S. government had to abandon the notion it could keep outsiders off its computer networks. "We've got the wrong mental model here," the director of the Information Systems Analysis Center at Sandia National Laboratories, testified. "I don't think that we would think that we could keep spies out of our country. And I think we've got this model for cyber that says, 'We're going to develop a system where we're not attacked.' I think we have to go to a model where we assume the adversary is in our networks. It's on our machines, and we've got to operate anyway. We have to protect the data anyway." Source: http://threatpost.com/en_us/blogs/inadequate-pay-outdated-approaches-and-bureaucracy-all-contribute-foreign-ownership-federal-sy

Report: In-app ads pose significant security risk. Researchers from North Carolina State University found that in-app advertisements pose privacy and security risks. In a recent study of 100,000 apps in the Google Play market, researchers noticed that more than half contained so-called ad libraries. And 297 of the apps included aggressive ad libraries that were enabled to download and run code from remote servers, which the researchers said raise significant privacy and security concerns. An assistant professor of computer science at the university and co-author of a paper describing the work, said in a statement that running code downloaded from the Internet is problematic because the code could be anything. "For example, it could potentially launch a 'root exploit' attack to take control of your phone –- as demonstrated in a recently discovered piece of Android malware called RootSmart," he wrote. Source: http://www.wirelessweek.com/News/2012/03/report-in-app-ads-pose-security-risk/

Data breaches increasingly caused by hacks, malicious attacks. A new study of data breaches found criminal and malicious attacks accounted for 37 percent of corporate data breaches in 2011, a 6 percent rise from 2010. The study, performed by Ponemon Institute and sponsored by Symantec, also found that these attacks were much more costly to companies than breaches caused by software or hardware failures or by internal negligence. More than two-thirds of malicious attacks were achieved through some sort of electronic exploit — only 28 percent involved the physical theft of data storage devices. The study also found that 33 percent of criminal and malicious breaches involved insiders. Source: http://arstechnica.com/business/news/2012/03/data-breaches-increasingly-caused-by-hacks-malicious-attacks.ars

Address spoofing vulnerability in iOS's Safari. Through a vulnerability in WebKit in the mobile version of Safari, an attacker could manipulate the address bar in the browser and lead the user to a malicious site with a fake URL showing above it. A security researcher published an advisory that explains the problem. Incorrect handling of the URL when the JavaScript method "window.open()" is used allows an attacker to "own" HTML and JavaScript code in the new window and, in turn, change the address bar. Fraudsters could use the vulnerability for phishing

attacks by sending users to pages that appear to be their bank and asking for account data. The vulnerability affects WebKit 534.46 in the latest iOS version 5.1, though earlier versions of iOS may also exhibit the problem. Users of third party browsers based on WebKit on iOS could also be vulnerable to the address spoofing. The researcher informed Apple of the problem in early March. Source: http://www.h-online.com/security/news/item/Address-spoofing-vulnerability-in-iOS-s-Safari-1476314.html

Beware of fake Google AV. According to GFI researchers, a number of pages offering "Google antivirus" software and threatening to block the users' access to Google services because of an infection have recently appeared, and they are listed among Google and Bing search results. The offered software is actually a rogue AV solution that has nothing to do with Google, and will likely try to bilk money from the victims. Currently, very few AV solutions detect the variant in question. Source: http://www.net-security.org/malware_news.php?id=2040&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+HelpNetSecurity+(Help+Net+Security)&utm_content=Google+Reader

Trial finds eight ways to defeat Google, PayPal and other SSOs. U.S. security researchers unearthed flaws in the single sign-on (SSO) services operated by a number of portals, including Google and PayPal. Idiosyncratic methods of integrating the APIs, SDKs, and sample code supplied by identity providers are creating exploitable security shortcomings, according to a study by two researchers at Indiana University and one Microsoft researcher. In particular, the researchers said, the process of token exchange is often mangled, which creates the possibility for attackers to sign into targeted accounts without having to crack an intended victim's password. The study — touted as the first field trial of popular Web SSO systems — focused on implementation problems rather than fundamental flaws in the cryptographic techniques at play, which are fundamentally fine. The exercise uncovered eight serious logic flaws in high-profile ID providers and relying party Web sites (which rely on authentication cookies to establish a user session). ID providers affected included OpenID (including Google ID and PayPal Access); Facebook; the JanRain platform; Freelancer; FarmVille; and Sears.com. Every one of the eight flaws allows an attacker to sign in as a targeted user. The researchers contacted the sites involved, which have largely deployed a fix. Source: http://www.theregister.co.uk/2012/03/20/sso_security_shortcomings/

Facebook 'cloaking' flaw allows unexpected snooping. A University College London research student and the chair of information communication technology told a conference of what they call a "zero day privacy loophole" in Facebook. Facebook users are not told when friends de-activate or re-activate accounts. That means trouble if the account is re-activated, as the newly re-activated friend regains access to anything their connections posted. Once they elicit information, they can de-activate the account again and their friends will almost certainly not know what happened or that they shared information. Source: http://www.theregister.co.uk/2012/03/20/facebook_deactivated_friend_zero_day/

Newly compiled driver shows Duqu authors still at work. One of the unique things about Duqu is the malware appears to be specifically tailored to each new victim. Rather than writing one

piece of malware and spreading it out to a large potential victim base, the crew behind Duqu had a small, specially selected group of targets, each of which got its own specifically crafted components and drivers. Researchers say the number of known victims of Duqu is small, perhaps fewer than 50. In the last several days, researchers at Symantec found a newly compiled driver for Duqu, leading to speculation the attackers are still tweaking and modifying their original work. March 20, one of the researchers who did the initial analysis of Duqu at Kaspersky Lab said while the new driver did not have any new functionality, there are indications it is not just new, but it is also aimed at evading existing detection techniques for Duqu. Source: http://threatpost.com/en_us/blogs/newly-compiled-driver-shows-duqu-authors-still-work-032012

Java-based Web attack installs hard-to-detect malware in RAM. Malware that does not create any files on the affected systems was installed onto the computers of visitors to news sites in Russia in a drive-by download attack, according to Kaspersky Lab. The attack code loaded an exploit for a known Java vulnerability, but it was not hosted on the affected Web sites themselves. Instead, it was served to their visitors through banners displayed by a third-party advertising service. The Java exploit's payload consisted of a rogue dynamic-link library (DLL) loaded and attached on the fly to the legitimate Java process. This type of malware is rare, because it dies when the system is rebooted and the memory is cleared. The malicious DLL loaded into memory acted as a bot, sending data to and receiving instructions from a command and control server over HTTP. In some cases, the instructions given out by attackers were to install an online banking trojan on the compromised computers. "This attack targeted Russian users. However, we cannot rule out that the same exploit and the same fileless bot will be used against people in other parts of the world: They can be distributed via similar banner or teaser networks in other countries," the researcher said. Source: http://www.computerworld.com/s/article/9225300/Java_based_Web_attack_installs_hard_to_detect_malware_in_RAM?taxonomyId=17

National Monuments and Icons

(Arkansas) **Flood threat closing some national forest sites in Arkansas.** National forest officials in Arkansas temporarily closed recreation area campsites on the Ouachita and Ozark-St. Francis National Forests as strong storms moved across the state, heeding the warning that days of heavy rain were expected the week of March 19. Weather reports predicted 6 inches or more of rain and potential flooding in some areas. Officials warned everyone to be on high alert for potential flooding throughout all areas of both national forests and said some roads and dispersed camping sites may also not be safe to use. Source: http://arkansasmatters.com/fulltext?nxd_id=520762

Postal and Shipping

Report: Cargo theft at all-time high due to improved data sharing. CargoNet announced the key findings of a detailed survey of cargo theft activity in the United States in 2011, Manufacturing.net reported March 22. The report shows a rise in cargo theft reporting and

underlines that the main driver of this trend is improvement in collaboration and data sharing between the insurance and transportation industries and law enforcement. The report includes information reported to CargoNet on the type of commodities most often stolen, theft incident locations, and additional analysis such as the time of day and day of the week when cargo is most often targeted. The 2011 report indicated 1,215 cargo theft incidents. Of the total incidents, 116 involved base metals, 229 involved electronics, 105 involved apparel and accessories, and 200 involved prepared foodstuffs and beverages. The most cargo theft incidents occurred on Fridays (227 incidents), Saturdays (202), and Sundays (198) at locations such as truck stops, carrier/terminal lots, and unsecured parking lots. The cargo theft report is available at CargoNet's Web site. Source: http://www.manufacturing.net/news/2012/03/reportcargo-theft-at-all-time-high-due-to-improved-data-sharing

Public Health

Congress probes fake pharmacies in connection with drug shortages. Members of Congress investigating shortages of crucial drugs are targeting nearly two dozen fake pharmacies allegedly set up solely to buy and resell the drugs at huge markups. Two Senators and one Representative sent letters March 21 to three individuals believed to have obtained licenses to operate a pharmacy and a prescription drug wholesale business in a "shell game" — to make money by taking advantage of the drug shortage crisis disrupting hospital and other patient care. The letters request detailed information by April 11 about the businesses and their purchases and resale of cancer and other lifesaving drugs. The letters state they have found evidence of pharmacies speculating by buying prescription drugs in short supply from legitimate wholesalers, transferring those medicines to their own wholesale companies, and then selling them to other gray marketers at exorbitant markups. "If it's not illegal, we're going to have to find a way to make it illegal, because this threatens virtually every person in the country," one Representative told the Associated Press. Laws vary by state, but generally wholesalers may only buy drugs from manufacturers or other licensed wholesalers. Drug shortages have been wreaking havoc in hospital pharmacies, forcing doctors to postpone chemotherapy and surgeries and to give patients treatments that may be less effective, have more serious side effects, or cost substantially more. The lawmakers' investigation found evidence of one transaction where a licensed pharmacy called Priority Healthcare bought a chemotherapy drug called fluorouracil for $6.77 per vial. A distributor it owned called Tri-Med America allegedly sold the cancer medicine to another company for more than 10 times the initial price — $69 per vial. Source: http://www.pittsburghlive.com/x/pittsburghtrib/business/s_787661.html

Transportation

(New York) **NYPD says Iran has conducted surveillance in NYC.** Authorities interviewed at least 13 people since 2005 with ties to Iran's government who were seen taking pictures of New York City landmarks such as the Brooklyn Bridge, a senior New York City Police Department (NYPD) official said March 21. Police consider these instances to be pre-operational surveillance,

bolstering their concerns Iran or its proxy terrorist group could be prepared to strike inside the United States, if provoked by escalating tensions between the two countries. The NYPD's director of intelligence analysis told Congress that New York's international significance as a terror target and its large Jewish population make the city a likely place for Iran and Hezbollah to strike. He testified before a House homeland security panel about the potential threat. Much of what he said echoed his previous statements on the potential threat, but he offered new details March 21 about past activities in New York. In May 2005, tips led the NYPD to six people on a sight-seeing cruise who were taking pictures and movies of city landmarks. In September 2008, police interviewed three people taking pictures of railroad tracks. In September 2010, federal air marshals saw four people taking pictures and videos at a New York heliport. Interviews with law enforcement revealed all the people were associated with the Iranian government, but they were ultimately released and never charged, the director said. Source: http://online.wsj.com/article/AP365b220a2c5349aabb17ab386703ff77.html

Water and Dams

(Indiana) **Former head of wastewater treatment plant charged with falsifying reports.** The former superintendent of a Michigan City, Indiana wastewater treatment plant is facing federal charges related to reporting and monitoring methods at the plant, it was announced March 21. The man was charged with three felony counts of making a false statement under the Clean Water Act, according to the U.S. attorney's office for northern Indiana. The charges cover the period from July 2007 through June 2010. He was also charged with failing to make a required report of a bypass of a treatment process before discharging waste streams into Trail Creek, which flows into Lake Michigan; selectively reporting only sample results that showed compliance with Michigan City's discharge permit and not reporting samples that showed non-compliance; and tampering with a monitoring method. The U.S. attorney's office alleged the man, in taking a daily sample of wastewater to test for E. coli, delayed taking the sample until the point in the treatment process when the treatment chemical (chlorine) was elevated and when E. coli concentrations would be at lower levels. Source: http://www.southbendtribune.com/news/sbt-former-head-of-wastewater-treatment-plant-charged-with-falsifying-reports-20120321,0,1321110.story

(Utah) **Vehicles stuck at Newton Rez spillway require Haz-Mat cleanup.** An SUV got stuck in the spillway of Newton Reservoir in northern Utah, sometime between March 17-18. Fire crews from Newton, Cache, and Smithfield responded to the area and soon called in the Bear River Health Department to assist in cleaning up gas and oil that spilled into the water. The assistant chief of the Newton Fire Department said the vehicle accessed the restricted area below the reservoir and became trapped in the deep water. Another vehicle attempted to remove the first vehicle and became stuck itself. Reservoir officials shut off the flow of water from the reservoir March 18. A local towing company completed the removal of the trapped vehicles while a small amount of gas and oil contaminated the water. Once the cleanup was complete, crews left the scene and the spillway was reopened. Officials said further investigation of the case and whether charges will be filed will be handled and determined by the Cache County

Sheriff's Office. Source: http://www.cachevalleydaily.com/news/local/Vehicles-stuck-at-Newton-Rez-spillway-require-Haz-Mat-cleanup-143140156.html

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168